ATRiM

Protecting critical infrastructure

Asymmetric threats are the new normal

There is no guaranteed way to eliminate all threats to critical infrastructure. Yet there are ways to drastically minimize them. ATRiM uses crime prevention science and our unique automated software to provide you with state-of-the-art prevention. Anti-Terror

ATRiM is specially developed for property owners, city administrators, facility managers, police and fire officials, security specialists, engineers, architects, and planners.

Protect your infrastructure

ATRiM is a new approach for protecting critical infrastructure. Our product is the first automated software – we call it the Anti-Terror Risk infrastructure Matrix – to employ a sophisticated audit matrix based on crime prevention science.

WE developed this product after years of hands-on experience and research in safety auditing and crime prevention through environmental design.

What is it?

OUR unique critical infrastructure protection software employs an audit technology to assess the risks to your infrastructure and vulnerable assets. We do this with a qualified ATRiM representative and key members of your organization to form an audit team. Our audits specifically focus on terrorism attacks and criminal threats.

THE audit team then uses ATRiM protocols loaded onto hand-held remote data collection devices. We then download the encrypted data for analysis.

Protecting your site in a robust way means analytical precision beyond simple checklists.

Asymmetric threats

THERE is no guaranteed way to eliminate all asymmetric threats – major emergency, crime or multiple forms of terror risks to critical infrastructures. There are ways to minimize those threats. The key is to avoid simplistic audits and instead employ a strategic response well in advance of an event. This is the purpose of ATRiM - the Anti-Terror Risk infrastructure Matrix.

WE created our software after years of developmental work in crime prevention science and anti-terrorism analysis. We combined the lessons of past experience with operational and physical vulnerabilities and wrote software that allows us to rate and rank precise areas of your infrastructure. This provides a fine grained assessment at a higher level than other auditing methods such as the CARVER method, ASIS security checklists, or regular CPTED audits.

How do we protect audit data?

ATRiM's analytical algorithm is the protected sole proprietorship of Gregory Saville and Nicholas Bereza of the ATRiM Group. No other organizations, governments, or corporations have access to the software at any time. All audit data is encrypted on handheld mobile data collection devices independent of the analytical software.

Second, we take steps for multiple redundancies to ensure that audit data are kept secure. Data is encrypted immediately at collection and remain so until transferred to the software for analysis. When we deliver your final report, your data can be secured in encrypted format or destroyed. The choice is yours.

Encryption protection

Data from audits is protected by encryption software. There is no outside access to the analytical algorithm at any time.

Finally, all your personnel on the audit team will have proper security clearance. Only persons you authorize will have access to your final audit report.

The ATRiM software includes potential for 3D visualization, assessments in both 1st and 2nd Generation CPTED, and full data encryption.

System Capacity

THE ATRiM software includes potential for 3D Visualization of the site, audit team CPTED assessments in both 1st and 2nd Generation CPTED, as well as Situational Crime Prevention, fast data entry, GPS point analysis, and camera, voice and text notes.

The software allows on site Quick Reference, with PDA's we provide during the site visits, automated multiple team data consolidation from multiple sites, and a graphical representation of a site strengths and weaknesses.

It provides full data encryption and an external report viewer without compromising the security of a single workstation.

We provide all system requirements during the audits. When annual audits are conducted on site, we provide the necessary tutorials, Quick References, and reference manual if required.

The ATRiM software includes potential for 3D Visualization of the site, audit team assessments combining 1st and 2nd Generation CPTED, as well as situational crime prevention, fast data entry, GPS point analysis, and camera, voice and text notes.

The software allows on site Quick Reference, with PDA's we provide during the site visits, automated multiple team data consolidation from multiple sites, and a graphical representation of a site strengths and weaknesses.

It provides full data encryption and an external report viewer without compromising the security of a single workstation.

The software provides full data encryption and an external report viewer without compromising security at a single workstation.

Major events have ripple effects

Cascade failures

CRITICAL infrastructures present some unique vulnerabilities, such as cascading and escalating failures. Cascading occurs when a criminal, terrorist, or security attack of one target can occasionally cascade to affect other similar infrastructures. Consider the case in 2003 of one failed transformer in the Ohio electricity generating station that knocked out the eastern seaboard power grid affecting 50 million residents.

EQUALLY damaging is when one failed infrastructure escalates onto other different kinds of infrastructures. For example, the destruction of transportation routes, such as roadways near hospitals, can escalate the impact on other infrastructures by preventing the delivery of emergency services.

Public image

THE public relations and image of a facility, service or organization can be irreparably damaged from being unprepared. This can affect service delivery and public confidence for years. Consider the catastrophic impact on the entire airline industry following the 9/11 terrorism.

Major crime or terrorism events can occur anywhere. Threat assessment and vulnerability analysis indicate the likelihood of an event, but not what to do about it. Only ATRiM risk audits do that.

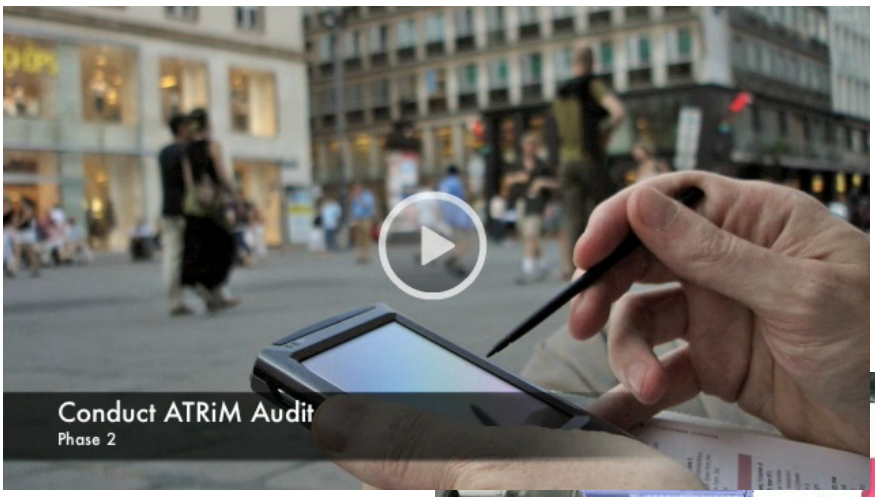
The critical infrastructure protection plan

Risk audits. This is the core of the risk assessment. It involves a look at the severity of attack and impacts from specific weaknesses in physical design and operational procedures. ATRiM is the most advanced risk assessment model of its kind.

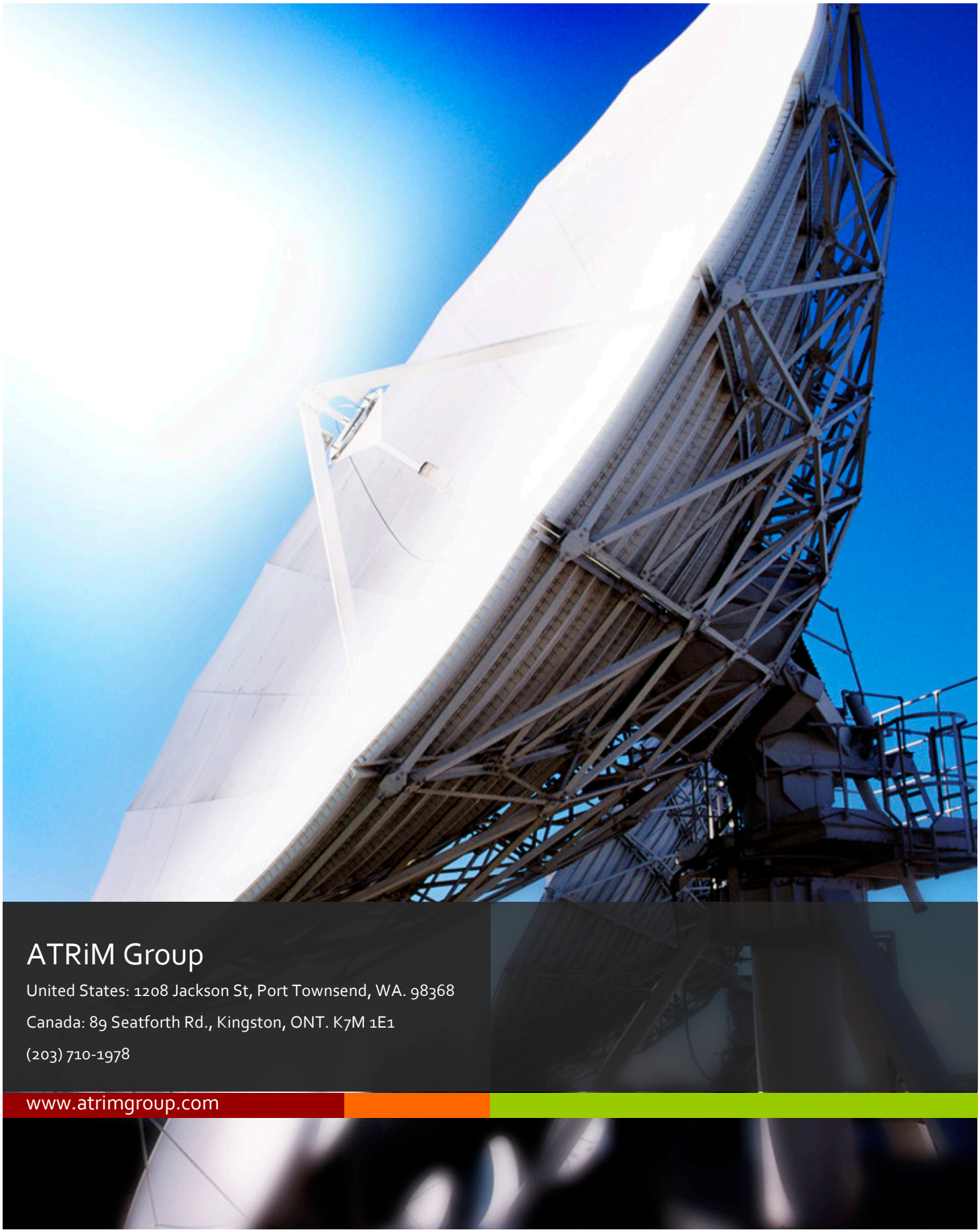
Asset appraisal. This includes an inventory of the existing vulnerable assets under consideration. This appraisal is context-based in that it depends on the potential targets existing at a site and their human and economic value. During the ATRiM process clients create their own inventory in order to complete audits.

Threat assessment. This deals with the likelihood and possible attack severity of a given target. It hinges on the ebb and flow of the current political climate or crime environment. It therefore relies heavily on reliable intelligence and police data, along with competent synthesis and analysis of that data.

Vulnerability analysis. This applies flaws in physical design and operations to potential for cascade failures, public relations, contagion, return-to-service lags, organizational morale, and replacement alternatives.



Risk audits represent the core of a competent critical infrastructure protection plan



ATRiM Group

United States: 1208 Jackson St, Port Townsend, WA. 98368

Canada: 89 Seatforth Rd., Kingston, ONT. K7M 1E1

(203) 710-1978

www.atrimgroup.com